AGENCY OF HUMAN SERVICES

AHS Continuous Monitoring Standard

Jack Green

10/9/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Security Monitoring (CA-7, CA-7(1), CA-7(2)) Controls.

Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
10/8/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements. Rev'd to 3.0 for consistency	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Security Monitoring (CA-7, CA-7(1), CA-7(2)) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

STANDARD

Continuous Monitoring

1. A continuous monitoring strategy must be established and implemented that includes the following:
    a. A configuration management process for the information system and its constituent components.
    b. A determination of the security impact of changes to the information system and environment of operation. The security state of the information system shall be assessed as the result of events that affect risks or indicate controls may not be adequate. These events include but are not limited to the following:
        i. An incident that results in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system.
        ii. A newly identified, credible, information system-related threat to organizational operations and assets, individuals, or other organizations is identified based on intelligence information, law enforcement information, or other credible sources.

iii. Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware or software.

c. The following actions are required during the assessment of the information system's security state:
    i. The Security and/or Privacy Manager must reconfirm the security category and impact level of the information system.
    ii. The Security and/or Privacy Manager may use independent security assessment agents or teams to monitor or assess VHC security controls on a periodic or ongoing basis
    iii. The Security and/or Privacy Manager must assess the current security state of the information system and identify risk to organizational operations and assets, individuals, or other organizations.
    iv. The Security and/or Privacy Manager must investigate the information system vulnerability (or vulnerabilities) exploited by the threat source (or potentially exploitable by a threat source) and the security controls currently implemented within the system as described in the security plan.
    v. Then, the Security and/or Privacy Manager plans for and initiates any necessary corrective actions based on the results of an updated risk assessment.
    vi. The AO will then determine and document if reauthorizing of the information system is required based on the severity of the event, the adverse impact on organizational operations and assets, individuals, or other organizations, and the extent of the corrective actions required to fix the identified weaknesses or deficiencies in the information system.
    vii. The security assessments performed are performed on a continuous and unannounced basis.

2. Monthly, quarterly, and annual reports on the security state of the information system to will be made available to the Security and Privacy Manager or CIO in accordance with continuous monitoring strategic and implementation plans.

3. The Security and Privacy Manager will review monthly, quarterly, and annual reports as provided and ensure corrective actions are implemented accordingly.

IMPORTANT INFORMATION

These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec